Aultech Privacy Notice

For Business Customers

Effective Date: **22 July 2025**

Contents

1. Introduction

This Privacy Notice explains how Aultech Proprietary Limited ("**Aultech**", "**we**", "**us**", or "**our**") collects and processes personal data as a data controller in relation to its enterprise SaaS platforms, including its products and offerings described on our website ("**the Services**"). The Services are exclusively provided to business customers and not to consumers or individuals in their personal capacity.

This notice complies with applicable laws such as South Africa's Protection of Personal Information Act 4 of 2013 ("**POPIA**"), the United Kingdom's Data Protection Act 2018, and/or the EU's General Data Protection Regulation ("**GDPR**").

2. Scope of this Privacy Notice

This Privacy Notice applies exclusively to **Service Data**.

"**Service Data**" refers to personal information processed by Aultech when establishing, operating, supporting, and maintaining the Services for business clients, including onboarding, account administration, billing, security monitoring, technical support, service analytics, platform updates, and customer communications.

"**Customer Data"** (i.e., data uploaded or processed by Customers and End Users via the Services such as documents, project data, emails, site instructions, or AI task queries) is governed by the Aultech Services Agreement and Data Processing Addendum ("**DPA**"), where Aultech acts as a data processor/operator.

Where Aultech processes Customer Data, Aultech acts as a data processor (or operator under POPIA), and processes such data strictly in accordance with Customer instructions. If you are a user authorised under a Customer's Account and have questions about your data, please contact your Account Admin, as they are responsible for managing your data under applicable data protection laws.

3. Contact Us

Aultech is the controller for the Service Data we process, unless otherwise stated.

- **Full name of legal entity**: Aultech Proprietary Limited (Company Reg No.: 2025/226086/07).
- **Designated Person**: Mr Ushir Maharaj (Information Officer)
- **Email address**: privacy@aultech.ai
- **Postal address**:

  13 Hillclimb Road,
  Westmead,
  Durban,
  KwaZulu-Natal,
  South Africa,
  3610

4. What Service Data We Collect

We collect and process the following categories of personal data as part of the Service Data :

- **Business Account Data**: Company name, registration number, VAT number, billing and subscription details.
- **User Identity & Authentication**: Names, business email addresses, telephone numbers, job titles, user roles, admin assignments, login credentials (hashed).
- **Billing & Payment Data**: Invoicing records, payment confirmations, refunds, and debit orders.
- **Technical & Device Data**:
  - Device IDs, IP addresses, browser types, operating system, session logs, access logs, error reports.
  - Server-side application logs collected through Elastic stack and Azure telemetry.
  - Hosting provider metadata (e.g., from Azure and Teraco) for internal diagnostics.
- **Communication & Support Logs**:
  - Customer service tickets, onboarding calls, training session records, troubleshooting interactions.
  - Email agent interaction metadata for those using the integrated agent features (optional depending on implementation phase)..
- **Integration Metadata**: Limited data from third-party integrations (e.g., Microsoft Outlook, Gmail and Workspace).

5. How We Collect Service Data

We collect Service Data through:

5.1. **Direct Interactions:** Registration forms, contract execution, subscription onboarding, user provisioning, customer support communications.

5.2. **Automated Technologies:**

(a) Application telemetry, API usage logs, agent activity , system diagnostics, and platform analytics.

(b) Our email agent, where enabled, may collect metadata and perform rules-based tagging, routing, or auto-responses based on criteria set by the user.

(c) When you interact with our website, we may collect technical and usage information automatically from your browser or device using cookies and similar technologies. This includes browsing data and Cookies.

For example, when you view our website, we can see:

- what you click,
- what you view,
- how long you spend on pages,
- your device and internet connection details such as: type of device you are using, IP address and details about your internet connection, technical details such as your screen size and the software you are using, such as your web browser,
- your country or region (not exactly where you are unless we ask permission), and
- your unique advertising or other identification numbers allocated to your browser or device.

(d) We don't often know exactly who you are from this data. But sometimes we may connect this data with other information we hold about you, for example, when you submit a 'contact us' form.

(e) Cookies and similar technologies are set on your device by us and our trusted partners, such as Google Analytics;

> To opt out of being tracked by Google Analytics across all websites, visit: http://tools.google.com/dlpage/gaoptout.

(f) Users can manage cookie preferences through our cookie consent tool.

5.3. **Third-Party Sources:**

We will only receive your personal data from third parties when (i) you have provided your consent to share such data with us, (ii) when required by law, (iii) when it is strictly necessary for us to fulfil our contractual obligations to you, or (iv) when it is strictly necessary to protect our or our Customer's legitimate interests, or (v) to protect the vital interests of the data subject. These circumstances may include, but are not limited to:

(a) **Third-party integrations**: Information processed from third-party integrations you set up with Aultech. For example, a third-party integration may give us access to information stored in that third party that Aultech will process to facilitate the integration;

(b) **Third-party payment processors**: When processing your payments via payment gateways or payment processors, we may receive confirmation of payment or refund details from these providers to ensure successful completion of your transaction, and

(c) **Companies Intellectual Property Commission, Companies House and other public sources**: Public sources are used solely for verifying customer information during onboarding. We implement safeguards to ensure no over-collection or misuse of publicly available data.

6. Why We Process Service Data

When we process Service Data for the purposes described below, we rely on the following legal grounds:

Category	Personal Data (Service Data Only)	Purpose of Processing	Legal Basis
Business Account Information	Company name, registration number, VAT number, billing address	Account setup, invoicing, contract management	Contractual Necessity
Authorised User Information	Name, business email address, phone number, job title, admin roles	Create authorised accounts, assign user roles, user authentication	Contractual Necessity
Billing & Payment Data	Invoices, payments, debit order processing via Netcash, billing disputes	Payment processing, managing billing records	Contractual Necessity
Technical & Device Metadata	IP address, device type, browser type, session ID, login timestamps	Security monitoring, fraud prevention, platform stability	Legitimate Interest
Platform Access & Usage Logs	Login activity, audit logs, admin changes, Elastic logs	Audit trail, system monitoring, access control audits	Legitimate Interest
AI & Task Automation Logs	Task-related metadata, rule-based triggers, email sync metadata, generated documents.	Automating task management, claims, and contract analysis	Legitimate Interest; Contractual Necessity
Feature Interaction Logs	Metadata about user interactions with Bob, Document Control, or the Email Agent	Improve agent reliability, troubleshoot issues, and optimise performance	Legitimate Interest
Security Event Data	Suspicious login attempts, CrowdStrike endpoint detections, WAF traffic events	Threat detection, incident response, protecting system integrity	Legitimate Interest; Legal Obligations (security compliance)
Support Communications	Support tickets, customer service records, technical issue logs	Providing customer support and resolving issues	Contractual Necessity
Integration Metadata (Service-Level)	Metadata from integrations (Microsoft Exchange, Google Workspace, Active Directory)	Enable user identity management and service integrations	Contractual Necessity
Marketing & Communication Preferences	B2B contact information, opt-out preferences	Customer communications, service updates, legal notices	Legitimate Interest (opt-out rights apply)
Anonymised Operational Analytics	Aggregated, non-identifiable service metrics (uptime, login volumes, platform stability trends)	Platform improvement, operational analytics	Legitimate Interest

Additional information

To achieve the above processing purposes, we may use algorithms to recognise patterns in Service Data, manual review of Service Data (such as when you interact directly with our billing or support teams), and aggregation or anonymisation of Service Data to eliminate personal data. We also use Service Data for internal reporting and analysis of our platform and business operations.

7. Consequences of Failure to Provide Personal Data

If we are required by law or contract to process certain personal data and you do not provide it (e.g., identification verification documents), we may be unable to:

- Deliver our services, including configuring, supporting, or facilitating any training;
- Fulfil our contractual obligations, such as onboarding, billing, or security-related requirements;
- Comply with certain legal or regulatory requirements to verify your identity.

In such cases, we may need to suspend or terminate our contract and/or business relationship with you, providing due notice and acting under the terms of the contract and applicable legislation.

8. Service Data We Share and Disclose

8.1. We do not sell Service Data.

8.2. We may share your Personal Data with Aultech Affiliates who perform technical services for us or on our behalf as Processors for the purposes listed under "**Why We Process Service Data**".

8.3. We do not share Service Data with companies, organisations, or individuals outside of Aultech except in the following cases:

(a) We share Service Data outside of Aultech when you or our customer choose(s) to procure a Third-Party Service through our platforms,

(b) With your administrator who you authorise to manage your organisation's account. For example, they may be able to:

- view your account and billing information, activities and statistics,
- change your account password,
- suspend or terminate your account access permissions,
- restrict your ability to delete or edit your information or privacy settings.

(c) for external processing. We share Service Data with trusted third-party providers to process it for us as we instruct them to and in compliance with this Privacy Notice and appropriate confidentiality and security measures. For example,

- our sub-processors may include infrastructure or security vendors with whom we have agreements in place to ensure equivalent data protection standards,
- billing data is shared with payment processors, while technical details may be shared with cloud service providers for troubleshooting purposes,
- Service Data is shared with our third-party providers when you request technical support services. We share the information you provide in the support ticket, and those providers may communicate with you or your administrator in that ticket, including providing updates and closing the ticket, and
- we share your contact details to enable communication and collaboration when you request professional services.

(d) for legal reasons. We share Service Data outside of Aultech when we have a good-faith belief that access to, or disclosure that Service Data is reasonably necessary to:

- comply with applicable law, regulation, legal process, or enforceable governmental requests,
- enforce applicable agreements we have entered with you, including to investigate potential violations, detect, prevent, or otherwise address fraud, security or technical issues, or
- protect and defend the rights, property or safety of Aultech, our customers, users, employees, contractors, suppliers, service providers, the public or any third party, as required or permitted by law.

(e) In the event of beta services or feature access, we may share anonymised Service Data internally or with designated support teams to troubleshoot and enhance functionality during testing.

(f) for potential business transfers. If Aultech is involved in a reorganization, merger, acquisition, or sale of assets, we will continue to ensure Service Data is kept confidential and give affected users notice before Service Data becomes subject to a different privacy policy or Controller, and

(g) in other ways as you direct us, from time to time.

9. Special Category Personal Data

We generally do not collect special category personal data (such as race, religious beliefs, or health information) as part of the Service Data unless it is required for specific legal purposes (for example, during legal disputes or regulatory compliance). When we do process such data, it will be with your explicit consent, or as otherwise permitted by applicable laws. Any processing of such data by the Customer remains the sole responsibility of the Customer under the Customer Agreement and DPA.

10. Children

Our Services are designed for business use only. We do not knowingly collect data relating to children under 18 years of age.

11. Where Service Data is Stored and Transferred

11.1. **Storage Locations**: Your Service Data will be primarily stored and processed in data centres in South Africa and the European Union.

11.2. **Cross-Border Transfers**: Personal Data may be transferred to and processed in the Republic of South Africa ("RSA"), where our personnel are located. We apply the same protections described in this Privacy Notice in all cases. Some Service Data may pass through Cloudflare as part of Aultech's perimeter security measures.

11.3. When transferring Personal Data outside the EEA or RSA, we comply with the following legal frameworks:

(a) **Adequacy decisions:** We may transfer data to countries that the European Commission, UK Adequacy Regulations, or the Swiss Federal Council have determined adequately protect the data.

(b) **Transfer Impact Assessments ("TIAs"):** Before transferring data to countries without an adequacy decision, we conduct TIAs to assess risks and implement necessary mitigation measures.

(c) **Standard Contractual Clauses ("SCCs"):** We use SCCs approved by the European Commission and the UK Information Commissioner's Office to ensure your data is adequately protected.

(d) **Data Encryption:** Where appropriate, we encrypt personal data before transfer to prevent unauthorized access or interception.

12. Security and Integrity

12.1. We take the security and protection of your Service Data seriously. In line with industry standards, we implement appropriate technical and organisational measures to prevent unauthorised access, accidental loss, destruction, or alteration of your Service Data. Our security measures include:

(a) **Access control**: Restricting access to employees, contractors and agents who strictly need it to perform their duties, all of whom are subject to strict confidentiality obligations. Use of third-party security tools to prevent malicious activity and unauthorised access attempts.

(b) **Encryption**: Encrypting Service Data at rest and while in transit,

(c) **Review and Testing**: Regularly reviewing our processing practices and systems for vulnerabilities and implementing updates and patches to secure our infrastructure. We conduct periodic data integrity tests and backup recovery simulations to validate the reliability of our disaster recovery procedures.

(d) **Incident management**: Implementing a response plan to address and mitigate any data breaches or security incidents. We may retain backup copies of customer data for up to 180 days to support operational resilience and disaster recovery

12.2. While we take all reasonable steps to protect your Service Data, you acknowledge that no system is entirely secure, and unauthorised access remains a potential risk in the digital world.

12.3. If we become aware of a data breach that compromises your Service Data, we will notify you and the relevant regulatory authorities in accordance with legal requirements.

13. Accuracy, Access and Portability of Service Data

13.1. We strive to ensure your personal data is accurate, complete, and up to date. It is your responsibility to inform your administrator of any changes to your personal data so they can update your records with us.

13.2. Your administrators can access user-specific data, such as account configurations and billing information, but access to sensitive data may be restricted based on role permissions.

13.3. Your employer may allow you to access and export your data to back it up or transfer it to a service outside of Aultech. To access and download the data you have stored in the services, please submit your request to our Information Officer by emailing privacy@aultech.com

14. Retention and Deletion of Service Data

14.1. **Retention Periods**: We will retain your Service Data as a Controller only for as long as it is necessary to fulfil the purposes for which it was collected, or as required by law.

14.2. **Determining Retention**: The retention period is determined by various factors, including:

(a) The type of data and its sensitivity.

(b) The purposes for which the data was collected and whether those purposes can still be achieved.

(c) How you configure your settings.

(d) Legal obligations that may require us to retain certain data for a specific period (e.g., tax laws, accounting regulations, or litigation holds).

14.3. **Deletion**: \You may request deletion of your Service Data following account termination or non-payment. We will permanently delete or de-identify such data within 30 days of termination, unless retention is required by law.

14.4. **Customer Instructions**: Certain data uploaded to and generated by our platform is retained or deleted based on the instructions provided by the customer, as the controller, and following our Enterprise Agreement and Data Processing Addendum. Where the email agent or Scout generates logs, these are retained for up to 180 days unless the customer instructs earlier deletion.

14.5. **Backup copies**: After we complete the above steps, copies of Personal Data may remain for a limited period in our encrypted backup systems, which we maintain to protect data from accidental or malicious deletion and for outage and disaster recovery purposes, before being overwritten by new backup copies.

14.6. **Service Downgrades or User Reductions**: Where a customer reduces the number of users on their subscription, data associated with the removed users may be archived or anonymised in accordance with the retention policy, but certain metadata may be retained for audit, billing, or legal compliance purposes.

15. Exercising Your Data Protection Rights

15.1. If South African, European Union, UK, or Swiss data protection law applies to our processing of your personal data, you may have certain rights, including:

(a) **Access**: Request copies of your personal data. Some exemptions may apply.

(b) **Rectification**: Ask us to correct inaccurate or incomplete information.

(c) **Erasure**: Request the deletion of your personal data in certain circumstances. Note that some Service Data (such as anonymised operational logs or AI interaction metadata) may no longer be attributable to any specific user and therefore cannot be modified or erased

(d) **Restriction**: Ask us to limit the processing of your data in certain circumstances.

(e) **Objection**: Object to processing based on our public tasks or legitimate interests.

(f) **Portability**: Request the transfer of your data to another organization or you. This is only applicable if processing is based on consent or contractual necessity.

15.2. Where applicable, self-service tools may be available to access, rectify, or delete your data directly from the platform. If these tools are not available, contact us at privacy@aultech.ai

15.3. There is no charge for exercising your rights, and we will respond within **30 calendar days**. We may ask for additional information to verify your identity and ensure the legitimacy of the request.

15.4. You also have a right to complain to the regulator in the country where you reside or operate, which may include:

Australia	Office of the Australian Information Commissioner	Oaic.gov.au
Botswana	Information and Data Protection Commission	bocra.org.bw
EU member state	Equivalent authority in any EU member state	edpb.europa.eu
Mauritius	Data Protection Office	dataprotection.govmu.org
Mozambique	Not yet established	portaldogoverno.gov.mz
South Africa	Information Regulator	Inforegulator.org.za
United Kingdom	UK Information Commissioner's Office	ico.org.uk/make-a-complaint/
Zimbabwe	Postal and Telecommunications Regulatory Authority of Zimbabwe	potraz.gov.zw

16. Links to Third Party Services

Our services may include links to third-party platforms or websites that we do not operate or control. Your interactions with these third-party services are governed by their respective privacy policies. We are not responsible for the privacy practices or security of external platforms.

17. Changes to this Notice

We may update this Privacy Notice to reflect new technologies, industry practices, regulatory requirements, or other purposes. If these changes are material, we will notify you as required by applicable law. Notice may be provided by email to your last known email address, by posting on our sites and platforms, or by other means consistent with applicable law. If you are participating in a beta service or pilot phase, we may provide separate or supplementary privacy disclosures applicable to those features.